Protecting America's Critical Infrastructure

The infrastructures that form the backbone of the American economy, including transportation, energy, water, chemicals, telecommunications and computers, and the food supply, remain highly vulnerable to terrorist attacks. Even though al Qaeda has made clear its desire to conduct catastrophic attacks that cause mass casualties and severe damage to our economy, the Administration has done little since 9/11 to improve the security of our critical infrastructures. It has not conducted comprehensive national risk assessments to prioritize spending or protective measures, created incentives for the private sector to invest in security, or developed standards to assist in measuring progress toward more secure infrastructure. To close the massive security gaps presented by our critical infrastructure, the Administration must vigorously engage the private sector with a sense of urgency and seriousness that has not been present to date and be willing to use all the tools at its disposal – cooperation, incentives, and, if necessary, regulation – to achieve a significantly greater level of security for the American people.

Al Qaeda has made it clear that attacking critical infrastructures within the United States achieves its dual aims of taking American lives and disrupting our economy. Late in 2001, Osama bin Laden boasted that the combined effect of the attack on New York, was "no less than one trillion dollars." Other tapes purported to be from bin Laden claimed that, "The youths of God are preparing for you things that would fill your hearts with terror and target your economic lifeline."[1]

While the United States has not suffered a terrorist attack since 9/11, the number of potential targets in the U.S. is nearly endless. For example, there are more than 7,000 U.S. chemical facilities where a toxic release could kill or injure over 10,000 people; an accident at any one of more than 120 of those facilities could threaten over one million people. The massive blackouts in the United States in August 2003, while not terrorism- related, demonstrated serious vulnerabilities in our electricity infrastructure. Transport systems of all sorts are particularly vulnerable to terrorist attack. The millions of rail and truck cars carrying toxic and combustible chemicals around the country daily are potential bombs on wheels. Every day, millions of citizens are potential targets at concentrated travel points like subway systems, train stations, and bridges and tunnels. Citizens are also vulnerable at concentrated public settings such as large buildings and public entertainment venues. Intelligence officials have warned of threats to water supplies and dams and of airplane attacks against nuclear facilities. Incidences of foot-and-mouth disease point out risks in the agricultural sector, while our ever-growing reliance on computers heightens the risk of cyberattacks.

[1] Peter Bergen, "Al Qaeda's New Tactics," *The New York Times*, November 15, 2002, A31.

Selected Infrastructure or Key Assets[2]	Asset Details
Agriculture and Food	87,000 food processing plants
Water	1,800 federal reservoirs; 1,600 municipal wastewater facilities
Public Health	5,800 hospitals
Telecommunications	Two billion miles of cable
Energy	2,800 power plants; 300,000 oil and natural gas producing sites; two million miles of pipelines
Transportation	120,000 miles of major railroads; 590,000 highway bridges; 500 major urban public transit operators; 5,000 public airports; 300 inland/coastal ports
Chemicals and Hazardous Materials	66,000 chemical plants, of which 12,000 are highly toxic and could put large numbers of Americans at risk in the event of terrorist caused release
Nuclear Power Plants	104 commercial nuclear power plants
Dams	80,000 dams
Large high volume structures	460 skyscrapers; 250 major arenas and stadiums

The Administration has not provided strong leadership to improve critical-infrastructure security. Indeed, according to The Brookings Institution, the Administration "largely ignores" major critical infrastructure in the private sector.[3] In testimony before the House Select Committee on Homeland Security (Select Committee), homeland security experts gave DHS "not a passing grade" on critical infrastructure protection.[4] In the area of critical infrastructure, the Administration is failing to adequately protect the homeland.

SECURITY GAP: Inadequate Incentives Exist to Promote Investments in Infrastructure Security.

To date, the extent of the Administration's policy to protect critical infrastructures is a nearly singular reliance on voluntary private action.[5] While the private sector – which owns 85 percent

[2] The list provided here represents selected infrastructure sectors and key assets. Other sectors and assets include emergency services in 87,000 U.S. localities; 250,000 firms in 215 distinct industries in the defense industrial base; 26,600 FDIC insured banking and finance institutions; 137 million postal and shipping delivery sites; 5,800 historic monuments and buildings; and 3,000 government-owned and operated facilities.

[3] Michael O'Hanlon, Peter Orszag, Ivo Daalder, et al, *Protecting the American Homeland: One Year On*, (Washington, DC: The Brookings Institution, 2002, with a new preface, January, 2003), xiv.

[4] Peter Orszag, Senior Fellow, The Brookings Institution, "Critical Infrastructure Protection in the Private Sector: the Crucial Role of Incentives," testimony before the House Select Committee on Homeland Security, joint hearing of the Subcommittee on Infrastructure and Border Security and the Subcommittee on Cybersecurity, Science, Research and Development, September 4, 2003.

[5] Office of Homeland Security, *National Strategy for Homeland Security*, (Washington, DC: the White House, July, 2002). According to the *National Strategy for Homeland Security*, private firms bear the primary responsibility for addressing public safety risks posed by their industries. See also, U.S. General

of critical infrastructure – must clearly play a crucial role in protecting critical infrastructures, "private markets by themselves do not provide adequate incentives to invest in homeland security."[6] Ultimate responsibility to provide for the common defense rests with the federal government. Policies that rest on the assumption that the private sector will provide sufficient critical-infrastructure protection will fail to provide adequate protection against the threats we face in an age of global terrorism.

The Administration's free-market approach to critical infrastructure is failing because, "the business of business is business, not homeland security," [7] and, "current [private sector] efforts fall woefully short of what is required."[8] Such shortcomings are acknowledged with respect to the chemical sector, for example. Secretary of Homeland Security Tom Ridge and former EPA Administrator Christine Todd Whitman both publicly voiced concern over the fact that chemical plants are attractive targets, stating that "voluntary efforts alone are not sufficient to provide the level of assurance Americans deserve," and chemical facilities "must be required to take steps" to improve security.[9]

Security is a collective good; consequently, in a purely free-market system, businesses simply do not have the economic incentives to invest in the level of security that society requires. Furthermore, "The ability of certain sectors to raise the necessary capital [for security enhancements] may be limited," and, "even sectors made up of large well capitalized firms are likely to make additional expenditures only if they can identify a net positive return on investment."[10] As a result of such economic realities, to the extent that private initiatives have been undertaken, they have been piecemeal within industries and uneven across infrastructure sectors.

The Administration must use all the policy tools at its disposal to change the structure of incentives to increase the critical infrastructure security of the United States. According to The Brookings Institution economist Peter Orszag:

> We must therefore alter the structure of incentives so that market forces are directed toward reducing the costs of providing a given level of security for the nation, instead of providing a lower level of security than is warranted.[11]

The need for using a full range of public policy tools, including incentives, is echoed by the GAO:

Accounting Office, *Homeland Security: Voluntary Initiatives are Under Way at Chemical Facilities, but the extent of Security Preparedness is Unknown*, GAO-03-439, March, 2003.

[6] Peter Orszag, Senior Fellow, the Brookings Institution, "Critical Infrastructure Protection in the Private Sector: the Crucial Role of Incentives," testimony before the House Select Committee on Homeland Security, September 4, 2003.

[7] Michael O'Hanlon, Peter Orszag, Ivo Daalder, et al, *Protecting the American Homeland: One Year On*, (Washington, DC: The Brookings Institution, 2002, with a new preface, January, 2003), xiv.

[8] Ibid, xxi.

[9] DHS Secretary Ridge and EPA Administrator Whitman, "A Security Requirement," *Washington Post*, October 6, 2002, B6.

[10] Congressional Research Service, *Critical Infrastructures: Background, Policy, and Implementation*, May 6, 2003, 25.

[11] Peter R. Orszag, Senior Fellow in Economic Studies, the Brookings Institution, "Critical Infrastructure Protection in the Private Sector: the Crucial Role of Incentives," testimony before the House Select Committee on Homeland Security, September 4, 2003.

> Last year, the Comptroller General testified … that the [DHS] would need to design and manage tools of public policy to engage and work constructively with third parties…. These [should] include grants, regulations, and tax incentives, and regional coordination and partnerships to motivate and mandate other levels of government or the private sector to address security concerns…. Without appropriate consideration of public policy tools, private sector participation in sector-related information sharing and other CIP efforts may not reach its full potential.[12]

The Administration's fiscal year 2005 budget request includes $200 million for targeted infrastructure protection grants (no funding was included in the President's budget request for fiscal year 2004).[13] Given the way in which such grants are currently used, however, the lasting benefits of such a program for increased infrastructure security are questionable. For example, of the $200 million in infrastructure protection grants provided in the fiscal year 2003 supplemental appropriation, nearly all of the roughly $60 million that has been spent to date went toward overtime pay for state and local law enforcement during the heightened terror alert before and during the Iraq War.[14] While critically important, such activities are reactive and temporary and do not improve the security of facilities over the longer term. Furthermore, due to weak government tracking of the program, DHS has to date been unable to provide information on the distribution of grant spending by infrastructure sector.

SECURITY RECOMMENDATION

To increase critical infrastructure security to an acceptable level, the Administration should explore tax incentives that promote increased investments in security by owners of critical infrastructure; seek to speed the development of affordable commercial products – including terrorism insurance and security assessment and audit products – that can help business owners increase security and also defray the potential costs of terrorist attacks; and work with owners of critical infrastructure, as necessary, to ensure a minimum regulatory framework that helps promote security in each of the critical infrastructure sectors without placing unreasonable burdens on business owners.

Examples of minimum regulations include requirements that critical infrastructure owners: carry terrorism-related insurance; undertake periodic vulnerability assessments against industry-determined best practices; and undergo periodic security audits, with such audits performed by independent and qualified third parties and judged against established objective benchmarks. Such measures will not only enhance security but can contribute to improving the safety, reliability, and performance of America's infrastructure sectors. Constructive investments in critical infrastructure sectors could contribute to economic growth, help individual business owners improve the quality and safety of their facilities, and improve the quality and reliability of our infrastructure nationally.[15]

(continued on following page)

[12] Robert Dacey, Director of Information Security Issues, General Accounting Office, written responses to posthearing questions from the September 17, 2003 hearing of the House Select Committee on Homeland Security, December 8, 2003.

[13] Department of Homeland Security, "Budget in Brief: Fiscal Year 2005," February, 2004.

[14] Office of Domestic Preparedness, briefing on the 2005 budget for members of the House Select Committee on Homeland Security, February 11, 2004.

[15] See the American Society of Civil Engineers, *Report Card for America's Infrastructure, 2003 Progress Report*, September, 2003, http://www.asce.org/reportcard which grades the general non-security-specific quality of U.S. infrastructures. Energy infrastructure received a D+; roads and bridges a D+/C; transit a C-;

The Administration must also ensure that any current or future grant funding for infrastructure protection is guided by an overall strategy, has stronger mechanisms to account for how it is used, and is accompanied by a better understanding of what is truly needed to improve critical infrastructure security in both the near and long term.

SECURITY GAP: A Comprehensive Risk Assessment of Our Nation's Critical Infrastructures Still Has Not Been Completed.

Given the enormity of the task of securing our critical infrastructures, it is imperative to conduct a comprehensive risk assessment in order to identify our greatest vulnerabilities and prioritize the implementation of protective measures. Despite the crucial importance of this task, the Administration has made little progress in developing a comprehensive national critical-infrastructure risk assessment.

According to the 2002 Homeland Security Act, DHS is required to comprehensively assess critical infrastructure vulnerabilities, prioritize protective measures, develop a comprehensive national plan for securing critical infrastructures, and craft policy to protect critical infrastructure.[16] Furthermore, the White House's *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* calls for DHS to identify key critical-infrastructure protection priorities and develop "an integrated critical infrastructure and key asset geospatial database."[17]

The potential risks of allocating limited homeland security resources in the absence of an informed risk assessment are apparent in the Transportation Security Administration's budget. In the fiscal year 2004 budget, 83.5 percent of the TSA budget was dedicated to aviation security, while only five percent went toward maritime and land transportation security.[18] In the fiscal year 2005 budget request, spending on maritime and land transportation fell below three percent of TSA's budget.[19] In the absence of a thorough and informed infrastructure risk assessment, we simply do not know whether such a disproportionate allocation of funds to aviation security makes sense. While aviation security should clearly be a priority, a full risk assessment might indicate that maritime and land transport deserve much greater attention. Trucks carry 68 percent, by weight, of all freight in the United States and they account for 82 cents on every dollar spent by U.S. businesses on shipping.[20] Furthermore, the National Intelligence Council and

---

drinking water a D; wastewater a D; dams a D; and hazardous waste a D+. Infrastructure that is outdated and in poor condition is more vulnerable to potential disruption, terrorism-related or not.

[16] Specifically, the Act, calls for DHS to: 1) Identify and assess the nature and threat of terrorist threats; 2) Understand such threats in light of actual and potential vulnerabilities; 3) Carry out comprehensive assessments of the vulnerabilities of key resources and critical infrastructure… including the performance of risk assessments to determine the risks posed by particular terrorist attacks within the U.S.; 4) Integrate relevant information, analyses, or assessments…in order to identify priorities for protective and support measures; 5) Develop a comprehensive national plan for securing key resources and critical infrastructures; and 6) To recommend measures necessary to protect the key resources and critical infrastructure

[17] Office of Homeland Security, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, (Washington, DC: the White House, February, 2003), 24.

[18] Congressional Research Service, "TSA Appropriations," memo to the House Select Committee on Homeland Security, November 4, 2003.

[19] DHS briefing on the 2005 TSA budget request for members of the House Select Committee on Homeland Security staff, February 9, 2004.

[20] American Trucking Association at www.truckline.com. See also www.truckersbestfriend.com.

leading homeland security experts view insecure ports and cargo containers as among the most likely means of weapons of mass destruction entering the United States.[21]

While the need for risk assessment as a crucial tool to prioritize efforts is widely accepted – even in the Administration's own strategy documents[22] – little has been done to perform the assessments. According to Governor James Gilmore, Chairman of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission), the Administration has written no less than eight homeland security strategies, and none of them were based on an adequate risk assessment.[23] "The lack of a comprehensive assessment of threats to U.S. infrastructures hampers defensive measures and preparedness activities."[24] Furthermore, the conference report on the 2004 Homeland Security Appropriations Act requested that DHS develop a "comprehensive risk analysis and assessments of vulnerabilities" of critical infrastructures "on a national scale" that will "focus on problems affecting multiple infrastructures."[25] The report language directed the Department to provide, by December 15, 2003, a detailed program plan, including scope, cost, and schedule for completing the plan. Although both DHS Undersecretary for Information Analysis and Infrastructure Protection, Frank Libutti, and Assistant Secretary for Infrastructure Protection, Robert Liscouski, pledged in congressional testimony to meet that deadline,[26] DHS has failed to deliver any plan to Congress. Instead, on December 17, the White House issued Homeland Security Presidential Directive 7 (HSPD-7), giving DHS yet another year to develop a 'plan' to develop a 'strategy' to identify, prioritize, and protect critical infrastructures. The Directive suggests that DHS is not getting the job done.

At a September, 2003 hearing before the Select Committee, testimony from DHS Assistant Secretary Liscouski cast serious doubt on whether the Administration is devoting adequate seriousness and attention to completing a comprehensive risk assessment in a timeframe that would allow such an assessment to inform critical programmatic and spending decisions.

---

[21] National Intelligence Council, *National Intelligence Estimate: Foreign Missile Developments and the Ballistic Missile Threat Through 2015,"* (Langley, VA: Central Intelligence Agency, December, 2001). See also Steven Flynn, Senior Fellow, Council on Foreign Relations, "Potential Strange Bedfellows? Homeland Security and Non-Proliferation in the Post 9-11 World," in *Monitor: International Perspectives on Nonproliferation*, September 18, 2003.

[22] See Office of Homeland Security, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, (Washington, DC: the White House, February, 2003). See also Governor James Gilmore, "Perspectives on 9-11: Building Effectively on Hard Lessons," testimony before the House Select Committee on Homeland Security, Sept 10, 2003.

[23] Governor James Gilmore, "Perspectives on 9-11: Building Effectively on Hard Lessons," testimony before the House Select Committee on Homeland Security, Sept 10, 2003.

[24] Gilmore Commission, "Implementing the National Strategy," Fourth Annual Report, (Arlington, VA: RAND, December 15, 2002), 84.

[25] According to House Appropriations Committee Report 108-169 on HR 2555, the DHS "will also develop a comprehensive risk analyses on a national scale that will be cross-sector in nature and focus on problems affecting multiple infrastructures…the Committee directs the Department to provide a detailed program plan outlining the proposed scope, total estimated cost, and schedule for completing the comprehensive risk analysis and assessments of vulnerabilities or the critical infrastructure. This plan is to be provided to the Committee by December 15, 2003."

[26] Undersecretary Libutti, testimony on DHS's Information Analysis and Infrastructure Protection Directorate, before the House Appropriations Committee, Subcommittee on Homeland Security, September 4, 2004. Assistant Secretary Liscouski, testimony on "Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection: the Electric Grid, Critical Interdependencies, Vulnerabilities, and Readiness," before the House Select Committee on Homeland Security, September 17, 2003.

> CONGRESSWOMAN SANCHEZ: So you are telling me that in a month and a half, we are going to have a list with all of the very critical infrastructure sectors and where that infrastructure is, and what type of protection we need to do for it, or how we are going to protect and what it is going to cost us, and a prioritization of that list…
>
> ASSISTANT SECRETARY LISCOUSKI: And I will shortly retire right after that too. No. I was really referring to the Liberty Shield list. The [list you refer to] is …really a continuous work in progress, [the] assessment of all the critical infrastructure throughout the United States. I did not mean to mislead you to think that we would have all that categorized in the next month and a half. **I would be surprised, frankly, if we had that done in the next five years** *[emphasis added]***.**[27]

Five years is too long to wait when the threats exist now. On February 23, DHS announced that it will create by December, 2004, a national database of all physical critical infrastructure, ranked by priority. This is a positive development, but is only the first step toward the development of a robust risk assessment that can be used to guide policy development and prioritize the allocation of resources to protect all of our vulnerable critical infrastructures.

SECURITY RECOMMENDATION

DHS, in coordination with the intelligence community, private sector experts, federally funded research and development centers and the national labs, should, as soon as possible, but not later than October, 2004, assemble an initial/draft national critical-infrastructure risk assessment. Such an assessment should include a full assessment of threats,[28] vulnerabilities and consequences and leverage, to the fullest extent possible, already-existing risk assessments that have been performed by many states, infrastructure sectors and federal agencies. The study should be updated and improved on an annual basis. Funding for the risk assessment should be clearly identified in the President's annual budget with clear accountability for the assessment residing with DHS.

Congress should establish and the President support an expert advisory panel to assess critical-infrastructure security and suggest strategies for the protection of the nation's critical infrastructures.[29]

---

[27] Assistant Secretary Liscouski, testimony on "Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection: the Electric Grid, Critical Interdependencies, Vulnerabilities, and Readiness," before the House Select Committee on Homeland Security, September 17, 2003.

[28] Gilmore Commission, "Implementing the National Strategy," Fourth Annual Report, (Arlington, VA: RAND, December 15, 2002), iv, 47, 84. According to the report: 1) the President should direct that the National Intelligence Council perform a comprehensive National Intelligence Estimate on the threats to the nation's critical infrastructure; 2) DHS should produce continuing, comprehensive "strategic" assessments of threats inside the United States; 3) DHS should have a robust capability to combine threat and vulnerability information.

[29] Ibid, 83.

SECURITY GAP: No Performance Critical Infrastructure Performance Metrics Have Been Developed to Measure Progress and Create Accountability.

According to the GAO, none of the Administration's homeland security strategies "indicates milestones" or "establishes performance measures" by which to measure or establish accountability for critical infrastructure protection.[30] Furthermore, according to the Gilmore Commission:

> One of the critical shortcomings in structuring programs and securing funds to protect critical infrastructures is the lack of risk-based models and metrics to help explain the value of protective measures in terms that public and private decision makers understand.[31]

The Department includes only limited performance metrics regarding critical infrastructure in its fiscal year 2005 budget request. Specifically, DHS is seeking to increase the amount of threat information that it makes available to infrastructure sectors. By the end of 2005, DHS has set a 25 percent target for the number of infrastructure "assets" and "components" that will have "threat level information completed for use by decision makers for optimal deployment of assets."[32] The initiative may mark positive movement toward measuring the Department's activities,[33] but it falls far short of what is required, namely, specific risk-based models and metrics that fully incorporate threats, vulnerabilities and consequences and can be used to evaluate progress toward increased security within and across each of the critical infrastructure sectors.

SECURITY RECOMMENDATION

The Administration should follow the recommendation of the Gilmore Commission that DHS "develop metrics for describing infrastructure security in meaningful terms, and to determine the adequacy of preparedness."[34] In this task, DHS should fully leverage the modeling and analytic capabilities of National Infrastructure Simulation and Analysis Center (NISAC) and work in concert with representatives from each of the critical infrastructure sectors.

The DHS should prepare an annual report card which assesses the state of preparedness of each of

(continued on following page)

[30] Robert Dacey, Director of Information Security Issues, General Accounting Office, written responses to posthearing questions from the September 17, 2003 hearing of the House Select Committee on Homeland Security, December 8, 2003.
[31] Gilmore Commission, "Implementing the National Strategy," Fourth Annual Report, (Arlington, VA: RAND, December 15, 2002), 85
[32] DHS, "Performance Budget Overview, Fiscal Year 2005, Congressional Budget Justification," February, 2004.
[33] Representative Christopher Cox (R, CA), Chairman of the House Select Committee on Homeland Security, has expressed interest in developing performance measures for DHS. See, for example, Office of Representative Cox, "Homeland Security Members Announce Performance Measures for the Department of Homeland Security," news conference and press release, November 19, 2003.
[34] Gilmore Commission, "Implementing the National Strategy," Fourth Annual Report, (Arlington, VA: RAND, December 15, 2002), ix, 85.

the critical infrastructure sectors against specific performance metrics. In addition, DHS should grant annual awards recognizing significant improvements or achievements in critical-infrastructure protection. Such programs can be a powerful tool for government to motivate private sector actors to enhance infrastructure security, as the public-relations impact of such assessments can be significant.

SECURITY GAP: Information Sharing Between Government and Owners of Critical Infrastructure Needs to be Improved.

The improvement of information sharing between the federal government and owners of critical infrastructure is essential in securing the country against terrorist attacks. The government cannot adequately assess infrastructure vulnerabilities or respond to events without the essential input of infrastructure owners. Threat information must be bolstered by reports of suspicious incidents at individual facilities, and, in the event of an attack, infrastructure owners will be leading players in response and recovery. For the United States to adequately protect itself, communications between all levels of government and owners of critical infrastructures must be robust, full, and open.

The Administration has made little progress in achieving effective information sharing between all levels of government and private owners of critical infrastructure. Relationships between the private sector and the federal government are largely *ad hoc*, and the Administration needs to provide stronger leadership to make these relationships more explicit, more trusted, and more institutionalized.[35]

Specifically, the Administration has done little to delineate the functions, relationships, and mechanisms for information sharing in coordination with the critical sectors. According to the Partnership for Critical Infrastructure Security, the federal government has "not developed a comprehensive architecture describing the functions, relationships, and mechanisms for "information sharing" in coordination with the critical sectors."[36] The lack of progress on this front is disappointing, especially since both the GAO and the Gilmore Commission identified and have called for such measures since at least 2002.[37] The GAO found that "none of the [levels] of

[35] Kenneth C. Watson, President and Chairman, the Partnership for Critical Infrastructure Security, written responses to posthearing questions from the September 17, 2003 hearing of the House Select Committee on Homeland Security, November 17, 2003. Robert Dacey, Director of Information Security Issues, General Accounting Office, written responses to posthearing questions from the September 17, 2003 hearing of the House Select Committee on Homeland Security, December 8, 2003. Gilmore Commission, "Implementing the National Strategy," Fourth Annual Report, (Arlington, VA: RAND, December 15, 2002).

[36] Kenneth C. Watson, President and Chairman, the Partnership for Critical Infrastructure Security, written responses to posthearing questions from the September 17, 2003 hearing of the House Select Committee on Homeland Security, November 17, 2003.

[37] Robert F. Dacey, the U.S. General Accounting Office, "Critical Infrastructure Protection: Significant Homeland Security Challenges Need to be Addressed," statement of before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, GAO-02-918T, July 9, 2002, 4, 20, 43. In particular, the GAO identified a number of critical infrastructure protection priorities, all of which implicate improved information and sharing and coordination: 1) Clear delineation of critical infrastructure protection roles and responsibilities for federal, state, local, and private sector actors; clarification of how critical infrastructure protection entities will coordinate their activities; 2) clear definition of interim objectives and milestones; 3) clear timeframes for achieving objectives; 4) establishment of performance metrics; 5) improvement in analytical and warning capabilities. See also, the

government perceived the current information-sharing process with the federal government to be effective… and the information that was shared was not perceived as timely, accurate, or relevant."[38]

On February 19, 2004, the Administration released an interim final rule to protect information about the nation's critical infrastructure from public disclosure.[39] It also created a critical infrastructure information office to receive voluntary information submissions from the private sector.[40] While these are positive steps, the rules are nearly two years late, as the Homeland Security Act required that such "procedures shall be established not later than 90 days after the date of enactment" of the Critical Infrastructure Information Act in January, 2002.[41] Furthermore, the ability of the rules to significantly improve information sharing remains unclear. Even if the new protections spur improved information flow from the private sector to DHS, the Department still lacks sufficient authority to require plant operators in vulnerable sectors to submit information or actually follow DHS advice and make security improvements. As a result, to significantly increase the level of information sharing "may also require the consideration of various public policy tools, such as grants, regulations, or tax incentives."[42]

SECURITY RECOMMENDATION

The Administration must improve information sharing between government and owners of critical infrastructure. Specifically, the Administration should develop a comprehensive national plan to facilitate the sharing of critical-infrastructure information that clearly defines roles and responsibilities of the DHS, other federal agencies, state and local governments, and private owners of critical infrastructure before, during, and after an attack on critical infrastructures. As part of such a plan, comprehensive procedures for information sharing should be established and

(Continued on following page)

Gilmore Commission, "Implementing the National Strategy," Fourth Annual Report, (Arlington, VA: RAND, December 15, 2002).

[38] Robert Dacey, Director of Information Security Issues, General Accounting Office, written responses to posthearing questions from the September 17, 2003 hearing of the House Select Committee on Homeland Security, December 8, 2003. See also GAO, *Homeland Security Efforts to Improve Information Sharing Need to be Strengthened*, GAO-03-760, August 27, 2003.

[39] The new regulations, promulgated under the 2002 Critical Infrastructure Information Act, are designed to address those fears by introducing an exemption from the freedom of Information Act. To qualify for the exemption, information about critical infrastructure must meet three criteria: it must be submitted by companies voluntarily; it must be information that they would not otherwise have to disclose to the government; and it must meet what the department calls 'the definition of critical infrastructure information in the act and the implementing rule.'

[40] Assistant Secretary Liscouski, testimony on "Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection: the Electric Grid, Critical Interdependencies, Vulnerabilities, and Readiness," before the House Select Committee on Homeland Security, Subcommittee on Infrastructure and Border Security and the Subcommittee on Cybersecurity, Science, and Research and Development, September 17, 2003.

[41] The Critical Infrastructure Information Act of 2002 within the Homeland Security Act of 2002, P.L. 107-296, Title II, Subtitle B, sections 211-215.

[42] Robert Dacey, Director of Information Security Issues, General Accounting Office, written responses to posthearing questions from the September 17, 2003 hearing of the House Select Committee on Homeland Security, December 8, 2003.

include the possible restructuring of interagency mechanisms.[43]

Additionally, the Administration should expand the Homeland Security Operations Center (HSOC) within DHS's IAIP Directorate to include on-site private-sector representatives from all major critical infrastructure sectors. Such inclusion of industry representatives will allow the HSOC to serve as a focal point for cooperation, trust-building, and education between and among critical infrastructure sectors and all levels of government. [44]

Finally, the Administration should create a new regime for security clearances that allows classifications for dissemination of intelligence and other information to private sector owners of critical infrastructure. A related training program for private sector officials to interpret intelligence products should be developed.[45]

[43] Ibid. Gilmore Commission, "Implementing the National Strategy," Fourth Annual Report, (Arlington, VA: RAND, December 15, 2002). Gilmore Commission, "Forging America's New Normalcy: Securing Our Homeland, Protecting Our Liberty, Fifth Annual Report, (Arlington, VA: RAND, December 15, 2003).
[44] Guy Copeland, Vice President, Information Infrastructure Advisory Programs, Computer Sciences Corporation and former Co-Chair, National Information Infrastructure Task Force, interview with House Select Committee on Homeland Security staff. Similarly, see the Gilmore Commission, "Forging America's New Normalcy: Securing Our Homeland, Protecting Our Liberty, Fifth Annual Report, (Arlington, VA: RAND, December 15, 2003), 16. which highlights the importance of significant and permanent state, local, and private sector representation within homeland security bodies responsible for intelligence assessment and incident management.
[45] Gilmore Commission, "Forging America's New Normalcy: Securing Our Homeland, Protecting Our Liberty, Fifth Annual Report, (Arlington, VA: RAND, December 15, 2003), 33.